REMARKS/ARGUMENTS

The Office Action of April 8, 2005 has been carefully reviewed and these remarks are responsive thereto. Claims 1, 3-7, 9, 11, 19-21, 23-28, 30, 33, 42, 67, and 69 have been amended, claims 12-18, 41, 50, 57, 58, and 71 have been canceled without prejudice or disclaimer, and new claims 74-78 have been added. Claims 1-11, 19-40, 42-49, 51-56, 59-70, and 72-78 thus remain pending in this application. Reconsideration and allowance of the instant application are respectfully requested.

The Office Action of April 8, 2005 rejected this application under the judicially created doctrine of obviousness-type double patenting over claims 10, 17, 24, and 31 of the application 10/691,841. Applicants are filing a terminal disclaimer herwith with regard to application 10/691,841 (Samji et al.). Accordingly, Applicant respectfully submits that all claims in this application are now allowable, as further discussed below.

Rejections Under 35 U.S.C. § 102

Claims 1-73 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Matsubara (U.S. Patent Appl. Publ. No. US 2003/0225796 A1). Applicants respectfully traverse this rejection for at least the following reasons.

In order to reject a claim as anticipated under 35 U.S.C. §102, a single prior art reference must teach every aspect of the claimed invention. MPEP § 706.02. Applicants have amended independent claim 1 to describe a method for sharing non-physical-folder items where information corresponding to the sharee and corresponding to the item to be shared is stored on the sharer's computer. Matsubara, in contrast, does not describe a method wherein sharing information for non-physical-folder items is stored on the sharer's computer. Rather, Matsubara maintains a virtual directory in a central server system. Matsubara, Abstract. Matsubara Figures 3 and 4, and the corresponding paragraphs 0039-0051, refer to a single file table and single directory table residing in a system server, which are accessible to all clients through network resource browser (NRB) software. Further, rather than "providing direct access from the sharee to the sharer," as recited in amended claim 1, Matsubara requires sharee clients to first interact with the server system.

Matsubara, Abstract. In paragraph 0062, Matsubara describes the communications that the sharee must have with the system server before gaining access to the sharer. The sharee interacts with the server to browse for files, check permissions to access the files, and learn the location of the files to be shared. Matsubara, paragraph 0062. Only then is the sharee able to contact the sharer. This is not the same as "direct access" as recited in amended claim 1. Dependent claims 2-11, 49, 55-56, and 70 are allowable for at least the same reasons as claim 1, as well as based on the additional features recited therein.

Applicants have also amended independent claims 19, 24, 33, 42, 67, and 69 to describe sharing methods and computer-program sharing requests involving "direct" communication from the sharee's computer to the sharer's computer. Thus, claims 19, 24, 33, 42, and 67 are allowable for at least similar reasons as claim 1. Matsubara requires sharee clients to first interact with the server system, rather than provide direct access from the sharee to the sharer. Matsubara, Abstract. Dependent claims 20-23, 25-32, 34-40, 43-48, 51-54, 59-68, and 72-73 are allowable for at least the same reasons as their respective base claims, as well as based on the additional features recited therein. Applicants respectfully request these rejections be withdrawn.

In addition, with respect to claim 4, Matsubara does not describe a method wherein if a file share already exists, the permissions on the file share are set so as to allow the sharee to access the item that is to be shared. Indeed, the terms "file shares" or "shares" are not mentioned anywhere in Matsubara. Rather, Matsubara teaches that access control list (ACL) permissions for directories and files reside in the directory and file tables of its RNS server. Matsubara, paragraphs 0043 and 0049. Matsubara further indicates in paragraph 0048:

> A file list field **410** specifies the files contained in this directory. The file list field can comprise a list of the internally generated file IDs **301** from the file table **300**, thus creating a link from the physical files to a subdirectory in the directory table (hence "file link"). Since the files physically reside on the various client systems;, [sic] the directory contained in the server system can be considered to be a virtual directory.

Thus, the directories in the directory table of Matsubara Figure 4 do not correspond to physical directories on a computer. Therefore, when Matsubara describes setting or checking

ACL permissions on these "directories," it refers only to sharing permissions within the Matsubara application. Matsubara assumes that the physical directory permissions are already set to allow sharees to access the shared items; Matsubara does not set the permissions on the *file share* so as to allow the sharee to access the item that is to be shared. In contrast, the Applicants in claim 4 recite a method that sets permissions on the *file share*, or the physical directory on the sharer's computer containing the files to be shared.

With respect to claim 7, Matsubara does not verify that the sharer's firewall will allow the sharee to access the shared item. Matsubara does not refer to firewalls, the detection of a firewall on the sharer's computer, or the configuration of a firewall to allow the sharee to access the shared item. Indeed, the term "firewall" is never even mentioned in Matsubara.

With respect to claims 9, 23, 30, 39, and 48, Matsubara does not describe a method or media comprising sending a link to the sharee. A sharee client in Matsubara is never sent a link from the server system or from a sharer client. The server system in Matsubara merely maintains a table of available files and directories, from which the sharee will connect to with NRB client software, to browse and select a file to access. Matsubara, paragraph 0062. Only after the sharee has selected a file, will the server system provide the location and credentials to access the file. Matsubara, paragraph 0066. The process described in Matsubara is similar to clicking a hyperlink while surfing the internet, in which one of ordinary skill in the art would not say that the user was "sent a link" by the publisher of the web site.

In contrast, the Applicants' specification states, "[I]n order to make items easy to find, the sharer can also have the system send to the sharee a link to access the shared items directly from the sharer's machine." Application, p. 4. Thus, the Applicants refer to actively sending a link directly to the sharee, rather than passively maintaining the directory structure and waiting for the sharee to access it and navigate to the link. Matsubara's brief reference to file links is simply not the same as sending a link to the sharee, as recited in claims 9, 23, 30, 39, and 48.

Similarly, with respect to claims 10, 31, and 40, Matsubara does not describe allowing the sharee to query the sharer's computer to see what the sharer has shared out with the sharee. As stated above, Matsubara only describes a method by which the sharee connects to a system server with NRB client software, to browse the list of sharable files. Matsubara does not

describe any method to query a specific sharer's computer. All information describing shared files for which sharee has permission to access will reside in the same hierarchy in Matsubara, in the system server and not on the individual machines of the sharers.

With respect to claims 56, 60, 62, 64, and 66, Matsubara does not describe sharing of non-folder non-file items, such as contact items or email items. The Office Action refers to paragraphs 0062, 0066, and 0068 when alleging that Matsubara is equipped to handle non-folder non-file items such as contacts or emails. However, the terms "contact," "appointment," "email," or "non-file" are not even in Matsubara. Further, it is not likely that the infrastructure described by Matsubara could support the sharing of these types of items. Non-file items do not reside within the physical file hierarchy of a computer, but are found in databases or data files associated with email programs, calendaring applications, etc. Matsubara creates and maintains a file table and a directory table in the server system, which store the location of the shared filed. Matsubara, figures 3 and 4. Since non-file items do not reside within the physical file system hierarchy of the computer, they would not have a VRL (virtual resource location) or other compatible format for storing the file location. Matsubara, paragraph 0051. Thus, Matsubara does not describe non-folder non-file items and, even if it provided some sort of suggestion, there is no expectation of success in modifying Matsubara to handle non-folder non-file items.

With respect to claims 70, 72, and 73, Matsubara does not describe a method or media comprising "determining whether the item is protected," or "determining whether to remove the protection." Matsubara maintains an ACL field to restrict the users that have permissions to access the sharable file. Matsubara, paragraphs 0043 and 0049. However, these permissions are different from the "protection" as claimed and as described in the Applicants' specification:

> In accordance with another aspect of the invention, the system resolves any issues with protection systems such as an encrypted file system (EFS) and digital rights management (DRM). In other words, in certain instances, a user may be sharing items that are protected by something like EFS. In this case, the system attempts to make sure that the items can be shared if such is allowed by the policy on the machine or the DRM on the item. Application, p. 3.

The Applicants' description of protection includes encrypted file systems, digital rights management systems, firewalls, and other types of system protection beyond mere permissions checking. Claims 70, 72, and 73 each recite detection of these types of system protection, and making the determination whether to remove the protection prior to sharing. This is not the same permissions checking done by Matsubara's access control lists.

Thus, Applicant respectfully requests the rejection of claims 1-73 be withdrawn.

New Claims

Applicant has added new claims 74-78, supported by the specification as filed. No new matter has been added. The new claims are allowable at least based on the allowability of their respective base claims, and further because the art of reference does not describe the use of virtual folders.

CONCLUSION

All rejections having been addressed, applicants respectfully submit that the instant application is in condition for allowance, and respectfully solicits prompt notification of the same. However, if for any reason the Examiner believes the application is not in condition for allowance or there are any questions, the examiner is requested to contact the undersigned at (202) 824-3153.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Dated this 8th day of July, 2005 By: /Ross Dannenberg/
Ross Dannenberg, Registration No. 49,024

1001 G Street, N.W.
Washington, D.C. 20001-4597
Tel: (202) 824-3000
Fax: (202) 824-3001

RAD/mmd